3 Module libre sur un anneau :

3.1 *Proposition :*

Soit A un anneau principal, E un A-module libre de rang fini, M un sous de E alors M est libre et $\text{rang M} \leq \text{rang E}$.

<u>Démonstration</u> :

Soit $e_1, e_2, ..., e_n$ une base de E, $e_1^*, e_2^*, ..., e_n^*$ la base duale de E^*

Soit E_i le module engendré par $\{e_1, e_2, ..., e_i\}$ et $M_i = M \cap E_i$

$e_i^*(M_i)$ est un sous module de A, c'est-à-dire un idéal de A ; comme A est principal, il existe $a_i \in A$ tel que $e_i^*(M_i) = Aa_i$

Si $a_i \neq 0$ soit $d_i \in M_i$ tel que $e_i^*(d_i) = a_i$

Soit $S = \{i \in [1, n]; a_i \neq 0\}$, et montrons que $B = \{d_i, i \in S\}$ est une base de M

B *est libre* :

$\sum_i = 0$ avec $c_i \in A$ pour tout $i \in S$, si les c_i ne sont pas tous nuls, soit i_0 le plus grand $i \in S$ tel que $c_i \neq 0$.

On a : $c_{i_0} d_{i_0} = -\sum\limits_{\substack{i \in S \\ i < i_0}} c_i d_i \in M_{i_0 - 1}$

$e_{i_0}^*(c_{i_0} d_{i_0}) = c_{i_0} e_{i_0}^*(d_{i_0}) = c_{i_0} a_{i_0} \neq 0$ car E étant libre, il est sans torsion.

$e_{i_0}^*\left(\sum\limits_{\substack{i \in S \\ i < i_0}} c_i d_i\right)_i = 0$ car $e_{i_0}^*(d_i) = 0$ pour tout $i < i_0$

Contradiction.

B est donc libre.

B *engendre* M :

Soit M' le sous module de E engendré par B.

Montrons par récurrence que $M' \supset M_i, \forall i$

On aura alors $M' \supset M_n = M$ et comme $M' \subset M$ $(\text{car } d_i \in M_i \subset M)$, on conclura que $M' = M$

a) $M' \supset M_1$?

Soit $x \in M_1 = M \cap E_1$ donc $x \in E_1$ et $x = ce_1$; $c \in A$

$e_1^*(x) = c \in e_1^*(M_1) = Aa_1$ donc $c = b_1 a_1$;

Deux cas peuvent se présenter :

(1) $a_1 = 0 \Rightarrow c = 0 \Rightarrow x = 0 \Rightarrow x \in M'$

(2) $a_1 \neq 0 : x = b_1 a_1 e_1$ or $d_1 = a_1 e_1$ car $d_1 \in Ae_1$ et $e_1^*(d_1) = a_1$, d'où $x = b_1 d_1 \in M'$.

b) Supposons $M' \supset M_{i-1}$ et montrons $M' \supset M_i$.

Soit $x \in M_i$, $e_1^*(x) = c \in e_1^*(M_i) = Aa_i$

Deux cas peuvent se présenter :

(1) $a_i = 0 \Rightarrow c = 0 \Rightarrow x \in \mathrm{M}_i \Rightarrow x \in \mathrm{M}'$.

(2) $a_i \neq 0 : c = ba_i$. Considérons l'élément $x - bd_i \in \mathrm{M}_i$

$e_1^*\left(x - bd_i\right) = ba_i - ba_i = 0 \Rightarrow x - bd_i \in \mathrm{M}_{i-1} \Rightarrow x - bd_i \in \mathrm{M}'$

Mais $bd_i \in \mathrm{M}'$ donc $\mathrm{x} \in \mathrm{M}'$.

3.2 ***Corollaire :***

Soit A un anneau principal, E un A-module engendré par un ensemble à n éléments ; M un sous module de E, alors M est engendré par un ensemble de cardinal inférieure ou égal à n.

Démonstration :

Soit le A-module libre A^n, $\left(e_i\right)_{1\leq i\leq n}$ sa base canonique et $f : \mathrm{A}^n \to \mathrm{E}$ l'application linéaire définie par $f\left(e_i\right) = b_i$ $\left(\left\{b_1, b_2, ..., b_n\right\}\right.$ étant un système générateur de $\left.\mathrm{E}\right)$.

f est surjective et $f^{-1}\left(\mathrm{M}\right)$ est un sous module de A^n.

Donc $f^{-1}\left(\mathrm{M}\right)$ est libre de base $\left\{d_1, ..., d_k\right\}$ avec $k \leq n$.

$\mathrm{M} = f\left(f^{-1}\left(\mathrm{M}\right)\right)$ est engendré par $\left\{f\left(d_1\right), ..., f\left(d_k\right)\right\}$.

3.3 ***Proposition :***

Soit A un anneau principal, L un A-module libre de rang n ; M un sous module de L de rang r, (donc $r \leq n$). Alors, il existe une base $\left(e_i\right)_{1\leq i\leq n}$ de L et une suite $\left(a_i\right)_{1\leq i\leq r}$ d'éléments de A tel que :

1. $\left(a_i e_i\right)_{1\leq i\leq r}$ est une base de M.
2. $a_i \mid a_{i+1}$ pour $1 \leq i \leq r-1$.

Les idéaux $\left(a_i\right)$ sont appelé facteurs invariants du sou module M par rapport à L et sont uniquement déterminés par la donnée de L et M.

Démonstration :

Nous montrons d'abord que si $\mathrm{M} \neq \{0\}$, il existe $e_1 \in \mathrm{L}$, $a_1 \in \mathrm{A}$, N sous module de L tel que :

$$\mathrm{L} = \mathrm{A}e_1 \oplus \mathrm{N}$$
$$\mathrm{M} = \mathrm{A}a_1\mathrm{e}_1 \oplus \mathrm{N} \cap \mathrm{M}$$

L'ensemble des idéaux $\left\{v\left(\mathrm{M}\right);\ v \in \mathcal{L}\left(\mathrm{L},\mathrm{A}\right)\right\}$ possède un élément maximal. Soit : $u\left(\mathrm{M}\right) = \mathrm{A}a_1$

Soit $e' \in \mathrm{M}$ tel que $u\left(e'\right) = a_1$.

Montrons que : $\forall v \in \mathcal{L}\left(\mathrm{L},\mathrm{A}\right) : a_1 \mid v\left(e'\right)$

Soit d le $PGCD$ de a_1 et $v\left(e'\right)$ donc :

$d = a_1 h + kv\left(e'\right) = \left(fu - kv\right)\left(e'\right) = w\left(e'\right) \in w\left(\mathrm{M}\right)$ avec $w \in \mathcal{L}\left(\mathrm{L},\mathrm{A}\right)$.

On a : $\mathrm{A}a_1 \subset \mathrm{A}d \subset w\left(\mathrm{M}\right)$ mais $\mathrm{A}a_1$ maximal parmi les

$v\left(\mathrm{M}\right)$, $v \in \mathcal{L}\left(\mathrm{L},\mathrm{A}\right)$ donc $\mathrm{A}a_1 = \mathrm{A}d$ et $a_1 \mid d \mid v\left(e'\right)$.

Soit $x_1, ..., x_n$ une base de L et $\left(p_i\right)_{1\leq i\leq n}$ les formes coordonnées $\left(\text{ie } p_i\left(x_j\right) = \delta_{ij}\right)$.

Comme $\mathrm{M} \neq \{0\}$, l'un des $p_i\left(\mathrm{M}\right)$ est non nul, donc

$a_1 \neq 0$ $\left(\text{sinon } \mathrm{A}a_1 \underset{\neq}{\subset} \text{ dans l'un des } p_i\left(\mathrm{M}\right) \neq \{0\}\right)$. Et ne serai pas donc maximal.

$a_1 \mid p_i(\text{e}')$ donc $p_i(\text{e}') = d_i a_1,\ d_i \in \text{A}$. Soit $e = \sum_{i=1}^{n} d_i x_i$ et l'on a donc $e' = a_1 e$, comme $u(e') = a_1 \neq 0$ on a $u(e) = 1$.Considérons alors :

$$\begin{aligned} p : \text{L} &\to \text{L} \\ x &\mapsto u(x)e \end{aligned}$$

$t(t(x)) = u(x)u(e)e = u(x)e = t(x)$. p est projecteur.

$\text{Ker}p = \text{Ker}u$, $\text{Im}\, p = \text{A}e$ et $\text{L} = \text{A}e \oplus \text{Ker}u$; $\text{Im}\,\text{A}e$ car $\text{Im}\, p \subset \text{A}e$ et $p(ae) = ae \in \text{Im}\, p$.

Soit :

$$\begin{aligned} p' : \text{M} &\to \text{M} \\ x &\mapsto u(x)e \end{aligned}$$

$u(x)e = \alpha\ a_1 e = \alpha\ e' \in \text{M}$

$p'^2(x) = p'(u(x)e) = u(x)e = p'(x)$

Donc p' est un projecteur et $\text{Im}\, p' = \text{A}a_1 e$ et $\text{Ker}p' = \text{M} \cap \text{Ker}u$. Ainsi $\text{M} = \text{A}a_1 e \oplus \text{Ker}u$

Nous montrons l'existence des a_i et e_i par réccurence sur le rang r de M .

<u>Si $r = 1$:</u>

Soit $e_1, e_2, ..., e_n$ une base de $\ker u$ $(\text{L} = \text{A}e \oplus \text{Ker}u)$,

$\dim \text{M} = 1 + \dim(\text{M} \cap \text{Ker}u)$ donc $\dim(\text{M} \cap \text{Ker}u) = 0$

Donc $\text{M} \cap \text{Ker}u = \{0\}$ donc $\text{M} = \text{A}a_1 e$. Ainsi $e_1 = e, e_2, ..., e_n$ est une base de L avec $a_1 e_1$ base de M.

Supposons le résultat vrai pour $r - 1$.

Soit M tel que $\dim\text{M} = 2$

$\dim\text{M} = 1 + \dim(\text{M} \cap \text{Ker}u)$ d'où $\dim(\text{M} \cap \text{Ker}u) = r - 1$; $\dim \text{Ker}u = n - 1$

$\text{M} \cap \text{Ker}u$ est un sous A-module de $\text{Ker}u$

Il existe donc une base $a_1, ..., a_r$ de A tel que $a_2 e_2, ..., a_r e_r$ base de $\text{M} \cap \text{Ker}u$,

avec $a_1 \mid a_{i+1}$ pour tout i, $2 \le i \le r - 1$

Or $\text{L} = \text{A}e \oplus \text{Ker}u$ donc $e_1 = e, e_2, ..., e_n$ base de L et $\text{M} = \text{A}a_1 e \oplus \text{M} \cap \text{Ker}u$

Donc $a_1 e_1, a_2 e_2, ..., a_r e_r$ base de M, il reste à montrer que $a_1 \mid a_2$:

Considérons $t \in \mathcal{L}(\text{L},\text{A})$ définie par $t(e_1) = t(e_2) = 1$ et $t(e_i) = 0$ pour $i > 2$

On a $a_1 = t(a_1 e_1) = t(e') \in t(\text{M})$ donc $\text{A}a_1 \subset t(\text{M})$ donc $\text{A}a_1 = t(\text{M})$, or $a_2 = t(a_2 e_2)$ donc $a_2 \in \text{A}a_1$ c'est-à-dire $a_1 \mid a_2$ CQFD.

3.4 ***Corollaire :***

Soit A un anneau principal, E un A-module de type fini. Alors E est isomorphe à un produit $\frac{\text{A}}{(a_1)} \times \frac{\text{A}}{(a_2)} \times \cdots \times \frac{\text{A}}{(a_n)}$ où les (a_i) sont des idéaux de A tels que $(a_1) \supset (a_2) \supset \cdots \supset (a_n)$.

<u>Démonstration</u> :

Soit $\{x_1, ..., x_n\}$ un système générateur de E.

On a un épimorphisme $\varphi : \text{A}^n \to \text{E}$

On en déduit : $\text{E} \simeq \text{A}/\text{Ker}\varphi$

A^n est un A-module libre et $\mathrm{Ker}\varphi$ est un sous module de A^n, par le théorème précédent, il existe une base $\{e_1, e_2, ..., e_n\}$ ¨de A^n, un entier $q \le n$ et des éléments $a_1, ..., a_q$ de A tel que

$\{a_1e_1, a_2e_2, ..., a_qe_q\}$ soit une base de $\mathrm{Ker}\varphi$ et que $a_i \mid a_{i+1}$; $1 \le i \le q-1$
Posons $a_p = 0$ pour $q+1 \le p \le n$; alors $A/\mathrm{Ker}\varphi$ est isomorphe au produit
des $Ae_i/Aa_i\, e_i$; $1 \le i \le n$.
Le résultat s'en suit en remarquant que $Ae_i/Aa_i\, e_i \simeq A/Aa_i$